MANNING CURTIS BRADSHAW
& BEDNAR PLLC
Jess M. Krannich (Utah Bar No. 14398)
jkrannich@mc2b.com
136 East South Temple, Suite 1300
Salt Lake City, UT 84111
Telephone: (801) 363-5678
Facsimile: (801) 364-5678

KIRKLAND & ELLIS LLP
Mark C. Holscher (*pro hac vice* forthcoming)
mark.holscher@kirkland.com
Diana Torres (*pro hac vice* forthcoming)
diana.torres@kirkland.com
Allison Buchner (*pro hac vice* forthcoming)
allison.buchner@kirkland.com
Kristin Rose (*pro hac vice* forthcoming)
kristin.rose@kirkland.com
Matthew Gamsin (*pro hac vice* forthcoming)
matthew.gamsin@kirkland.com
333 South Hope Street
Los Angeles, CA 90071
Telephone: (213) 680-8169
Facsimile: (213) 680-8500

Attorneys for Plaintiff Complete Merchant Solutions, LLC

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION

COMPLETE MERCHANT SOLUTIONS, LLC, a Utah Limited Liability Company, Plaintiff, v. FEDERAL TRADE COMMISSION, Defendant.	**COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF** Case No. 2:19-cv-00963-CMR Magistrate Judge Cecilia M. Romero

Plaintiff Complete Merchant Solutions, LLC ("CMS" or "Plaintiff"), by and through its undersigned counsel of record, hereby brings the following Complaint and alleges as follows:

PRELIMINARY STATEMENT

1. CMS brings this action to obtain a declaration and an injunction to stop the Federal Trade Commission ("FTC") from continuing to threaten and engage in conduct that is not only unfair and harassing but also far beyond the express limitations of its jurisdiction and enforcement powers. As a start-up founded in 2008 and still located in Orem, Utah, CMS is an Independent Sales Organization ("ISO") for several banks, helping those banks grow their businesses by identifying and helping to onboard businesses for which those banks process payments. CMS also develops merchant technology solutions to facilitate e-commerce. Many of its software products incorporate features to help merchants identify compliance and fraud risks—for example, a rogue sales agent or marketing affiliate whose behavior may mislead customers about their purchases, resulting in requests for refunds or "chargebacks." CMS has won several awards, been recognized nationally and regionally, has attracted investment from blue-chip private equity funds, and provides work to a force of nearly 300 employees and independent contractors, while serving more than 5,500 merchant accounts that together process over $3 billion in payments annually through the banks with which CMS partners.

2. To become an industry leader, CMS has for years invested millions of dollars to reduce the chance that it provides its services to any dishonest merchants. As a reflection of that investment, CMS currently has a "chargeback" rate, i.e., the rate at which customers' disputes about charges on their credit card bills are upheld (or not contested by the merchant), of .23%, far below the guideline provided by the major payment card brands of 1%. As is inevitable for any ISO in CMS's industry, however, a small number of merchants have misused their merchant accounts and employed a variety of techniques to try to defeat the measures used by CMS and

the banks to identify problem merchants. CMS bears the risk in those cases, and in many of those instances, CMS has borne not just risk, but the financial burden of those merchants' misdeeds, suffering the entire monetary loss while reimbursing the consumers for any chargeback liabilities that the merchants themselves did not cover.

3. Nonetheless, for the past two years, the FTC has submitted a barrage of Civil Investigative Demands ("CIDs" or in the singular, "CID") to CMS, purportedly under provisions of the FTC Act, 15 U.S.C. § 45(a) and § 53(b), seeking vast amounts of information relating almost entirely to a handful of businesses which CMS and its sponsoring banks ceased working with years ago. In an attempt to resolve this matter and convince the FTC that its focus is misguided, CMS has produced over 45,000 documents—totaling over 475,000 pages—responded to numerous interrogatories, and produced multiple employees for depositions, all at a significant cost to CMS and its business.

4. But the FTC does not really want the information it seeks, nor is it seeking to enforce the applicable standards. What it wants instead is to outlaw entire industries that it deems to be "high risk." To accomplish this goal, the FTC has *not* sought new legislation from Congress or pursued an open notice-and-comment rulemaking process. Rather, it has been targeting ISOs for the past several years through litigation, trying to prevent them from providing services for a wide variety of businesses, including businesses that use telephone marketing, businesses that teach people how to start new businesses or earn money in a new career, businesses that offer discounted prices on products such as vitamins and supplements purchased through a subscription, and businesses that provide computer technical support to consumers.

5. For the past two years, CMS has, unfortunately, been one of the ISOs caught in the FTC's crosshairs. FTC staff have threatened repeatedly to bring litigation against CMS and to

seek disgorgement from CMS of every dollar of revenue that certain of its former clients processed—regardless of whether the customers of those clients were dissatisfied, regardless of how long ago the challenged conduct occurred, and regardless of the fact that CMS themselves never actually handled any of the payments processed for these merchants. Under payment systems rules, only the acquiring bank, and not an ISO like CMS, ever has possession of those payments. To avoid potentially crippling litigation with the FTC demanding money *CMS never even touched*, the FTC has demanded that CMS agree to stop working with any business that the FTC considers "high risk." The FTC's demands, however, are so sweeping that they effectively would require CMS to stop working with merchants like Amazon, because Amazon offers "Subscribe & Save" deals on multivitamins and dietary supplements, and Best Buy, because Best Buy's Geek Squad offers computer technical support services.

6. Under the FTC Act, the FTC has the authority to police unfair business practices, but the vague term "unfair" does not confer upon the FTC the power to make banks' ISOs vicariously liable for failing to prevent merchants from committing fraud whenever the FTC claims (with the benefit of hindsight) that something more could have been done to prevent the fraud—nor does it grant the FTC the power to enforce such views through litigation. Congress, indeed, limited the definition of unfairness to require harm to consumers that cannot reasonably be avoided, but there can be no harm to consumers here because consumers who use bankcards can submit chargebacks and get refunded by acquiring banks and ISOs if they believe they have been harmed. The FTC has no authority whatsoever to eject thousands of law-abiding merchants—which themselves are *not* the subject of any legal action—from the payment systems on which they depend based on nothing more than the FTC staff's biases against particular industries. What the FTC seeks to do penalizes merchants who, in the vast majority of cases, are not the

subject of any legal action or investigation and makes it impossible for merchants in lawful industries to find the ISO services they need to process payments through banks because of the risk of liability. And the FTC has no business threatening to use powers that it does not have to bully legitimate ISOs into being complicit with its improper agenda or risk the onslaught of aggressive, protracted and expensive (not to mention meritless) litigation. The FTC is expressly prohibited from regulating banks, whose relationships with ISOs are regulated by the FDIC and other banking regulators, and is seeking an end-run around this limitation of its authority by going after the ISOs—who act as a sales arm for the acquiring banks, and are there to simply facilitate the connections between merchants and banks, the entities responsible for the processing of merchant transactions.

7. This Court should put an end to the FTC's overreach and threatened legal claims, grant CMS's request for declaratory relief, and issue an injunction prohibiting the FTC from bringing (or threatening to bring) any action against CMS in connection with the provision of its ISO services as described herein, premised on a violation of 15 U.S.C. § 45(a) or § 53(b), as such statutes give the FTC no authority to bring such actions.

JURISDICTION AND VENUE

8. This is an action for declaratory and injunctive relief pursuant to 28 U.S.C. § 2201 relating to an actual controversy arising under 15 U.S.C. § 45(a) and 15 U.S.C. § 53(b).

9. This court has subject-matter jurisdiction under 28 U.S.C. § 1331 because the action arises under the laws of the United States and 28 U.S.C. § 1337(a) because the controversy arises under the Federal Trade Commission Act.

10. Venue is proper under 28 U.S.C. § 1391(b)(2), 28 U.S.C. § 1391(b)(1) and (c)(2), 5 U.S.C. § 703, and 15 U.S.C. § 53(b).

11. Intra-district assignment to the Central Division is proper because the facts underlying the controversy occurred predominantly in Utah County.

PLAINTIFF

12. CMS is a limited liability company organized under the laws of the State of Utah, with its principal place of business located at 727 North 1550 East, 3rd Floor, Orem, Utah 84097.

13. CMS is an ISO for Commercial Bank of California (formerly National Bank of California), Chesapeake Bank, Deutsche Bank, Merrick Bank, and Wells Fargo. CMS was formerly an ISO for HSBC Bank. As an ISO, CMS acts as a sales agent of the banks that offer merchant payment accounts (known as "acquiring banks"), by referring merchants to the banks and helping the banks manage their customer relationships with those merchants.

14. CMS was founded in 2008 by Trever Hansen, Kyle Hall, and David Decker, all former merchant-level salespeople who realized that the industry was moving too slowly to keep up with the new digital era. From soon after its founding, CMS focused on serving start-up technology companies, such as e-commerce businesses, which at the time found it difficult to establish relationships with banks and payment processors because many acquiring banks refused to accept e-commerce customers.

15. Over the past decade, CMS has grown from a tiny start-up to a highly successful company, attracting investment from major private equity funds and winning numerous awards, including being listed on INC Magazine's list of 500 fastest growing companies in 2012 and 2013, Utah Valley Magazine's list of 50 fastest growing companies in 2012 and 2013, and as one of the Nilson Report's Top 50 Processors in 2017. CMS currently supports more than 5,500 merchant accounts and provides work for nearly 300 employees and independent contractors.

DEFENDANT

16. Defendant Federal Trade Commission is an independent agency of the United States. 15 U.S.C. § 41. Among the statutes it administers is Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a), which tasks it with preventing "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce," but excludes from its authority the regulation of banks. 15 U.S.C. § 45(a)(1) and (2).

FACTUAL OVERVIEW

17. Businesses small and large across Utah and the nation depend on access to convenient bankcard payment systems to support their daily operations. Consumers likewise depend on merchants' ability to accept bankcards to purchase a wide range of goods and services, often from the comfort of their own homes. Unlike cash, checks, or bank transfers, card payments give consumers additional confidence because they come with the guarantee that consumers will not bear the costs of fraud or packages lost in the mail. That is because the banks that offer merchant payment accounts (known as acquiring banks) and the service providers that work on the banks' behalf to refer merchants to the banks (i.e., the ISOs) each act as a guarantor when a consumer disputes a charge. That means that if the merchant cannot or will not pay a disputed charge (in industry jargon, a "chargeback") that was either upheld or that the merchant did not contest, the acquiring bank (i.e., the bank with whom the merchant has a merchant payment account) must do so. Those banks, in turn, require their ISOs to indemnify them for every cent of chargebacks.

18. Because acquiring banks and ISOs (like CMS) are liable for financial losses associated with chargebacks, they have a strong incentive to weed out merchants who abuse the privilege of access to payment systems. Catching bad actor merchants presents challenges: merchants who lie to customers have few qualms about lying to their banks and ISOs too; these bad actors often

make improper claims verbally or by telephone, where it is harder for banks and ISOs to spot them; and banks and ISOs often have difficulty determining whether claims merchants make are adequately substantiated or not. Over time, banks and ISOs have used increasingly sophisticated measures to vet merchants when they apply for a merchant account, and then to monitor their transactions on an ongoing basis to try to identify fraudulent merchants or merchants who try to evade anti-fraud controls.

19. As modern technology has allowed businesses to scale up and often operate with very limited brick-and-mortar presence, the diligence needed to identify bad merchants has had to evolve rapidly too. Payment associations like MasterCard and Visa, acquiring banks, and ISOs have worked actively to improve their diligence, and state and federal banking regulators like the FDIC require banking examiners to check that acquiring banks have programs in place to manage risks associated with merchant processing.

20. In recent years, however, a new player has arrived on the scene. The FTC is forbidden by statute from regulating banks. 15 U.S.C. § 45(a)(2). Nonetheless, it has deployed increasingly aggressive interpretations of its authority to prevent "unfair . . . acts or practices in or affecting commerce," 15 U.S.C. § 45(a)(1), to target acquiring banks' service providers and agents—particularly ISOs—for frauds committed not by the banks' service providers or ISOs themselves but by a small number of dishonest merchants for which the banks process payments.

21. The FTC Act does not provide for the vicarious liability of payment system participants for frauds committed by merchants. Unlike other federal statutes such as the Consumer Financial Protection Act and the Securities Exchange Act, its text does not even discuss liability for assisting a violation. *See* 12 U.S.C. § 5536(a)(3); 15 U.S.C. § 78t(e).

22. Nonetheless, in recent years, the FTC has begun taking the position that it is an unfair practice under the FTC Act for an ISO *to fail to prevent a merchant from committing fraud*. It has taken this position in spite of limitations Congress passed on the FTC's power to declare conduct as "unfair" in the wake of prior attempts to overreach into policy matters best left to Congress or to the expert agencies Congress intended. It has taken this position ***not*** through notice-and-comment rulemaking, which might allow affected persons to comment or to challenge the rule under the Administrative Procedure Act, but rather through threats to seek ruinous penalties through an action nominally for an injunction under Section 13(b) of the Act. 15 U.S.C. § 53(b). And the FTC does so here despite its inability to articulate any specific facts showing that CMS has violated, is violating, or is about to violate any law.

HOW BANKCARD PAYMENTS WORK

23. Millions of times every day, a consumer presents a credit card to pay for goods and services, and a series of transfers of data and money occur to make sure that the consumer gets the good or service purchased and the merchant gets the money for the transaction.

24. First, the merchant submits a request to receive a valid authorization of available funds to be transferred by transmitting an encrypted authorization data request to an acquiring bank's internal or external processor, such as Fiserv (formerly First Data), TSYS, Chase for Business, or Elavon.

25. Then, the acquiring bank or its processor transmits the data to the payment association networks, such as Visa or MasterCard, which in turn transmit the data to the individual cardholder's issuing bank.

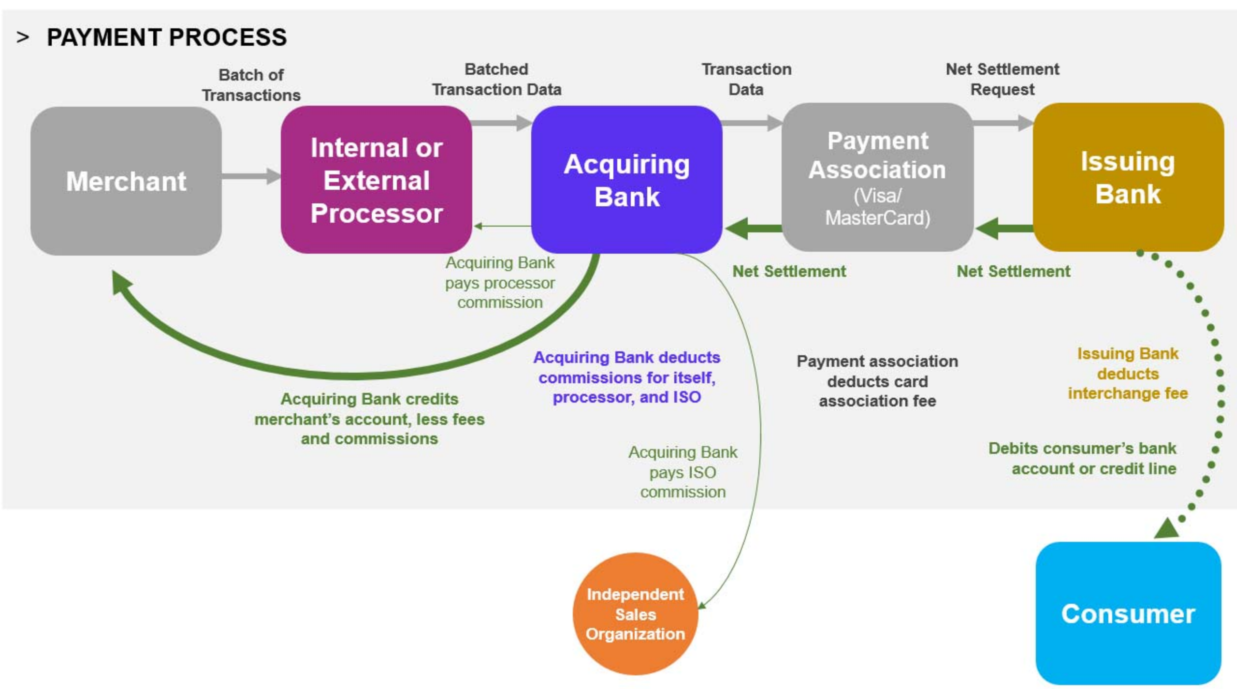
26. The issuing bank then either authorizes the amount and sends an authorization code to Visa or MasterCard, or declines the transaction.

27. The Visa or MasterCard networks then notify the acquiring bank or its processor whether the transaction has been authorized, which then inform the merchant.

28. At the end of the day, the merchant submits batches of transactions for payment to its acquiring bank either directly or through its merchant processor.

29. The acquiring bank then sends the transaction data to the payment association network, which determines the net amount of money that needs to be sent from the issuer's bank to the acquirer's bank, through a settlement and process commonly conducted by ACH or Fedwire.

30. Once the payment has cleared, and pursuant to the terms of the merchant's contract, the acquiring bank credits the merchant's account, minus the fees that the merchant owes to the cardholder's issuing bank ("interchange fee") and the card associations ("card association fee" or "assessments"), and the commissions charged by the acquiring bank, the merchant processor, and the ISO. The process summarized above can be depicted as follows:



31. ISOs generally do not have a role in the payment transmission or funding process; under payment association rules, it is a strictly held policy that only banks that are members of the

payment association can actually touch the money. Rather, as their name suggests, ISOs (like CMS) are merely sales organizations for the bank, paid by the acquiring bank for referring the merchant and performing ongoing customer service functions with the merchant.

32. Under payment association rules, it is the acquiring bank that has a duty to underwrite, oversee, control, and monitor its merchants, and which is responsible to the payment association if a merchant violates payment association rules. For example, VISA's Global Acquirer Risk Standards provide:

5 Merchant Underwriting and Onboarding

The merchant underwriting process is an important step in managing merchant risk. Whether merchants are solicited directly by the acquirer or through third party agents (such as ISOs and payment facilitators), all merchants must essentially be assessed for risk exposure. **The acquirer is always and solely responsible for the merchants it provides with card acceptance privileges**. If the acquirer allows third party agents to underwrite and board merchants, it is the acquirer that still is ultimately responsible **and it must have a control environment in place to ensure merchant underwriting is carried out in accordance with the policies and procedures set by the bank**.

33. Several functions of acquiring banks cannot be delegated to agents such as ISOs at all, including accepting merchants, signing the merchant agreement, possessing settlement funds, and holding any reserve funds withheld from the settlement funds. For example, VISA's Global Acquirer Risk Standards provide:

4.11 Merchant Settlement Responsibility

The merchant agreement must state the acquirer is responsible for providing settlement funds directly to the merchant.

The security and handling of merchant funds is a fundamental acquirer responsibility. This function cannot be delegated to a third party agent or other non-member entity, with the exception of a payment facilitator. Merchants must clearly understand that acquirers have direct responsibility for settlement. They must also be advised that agents are not permitted to directly access or hold merchant funds, whether from settlement or reserves.

6.1 Acquirer Reserve Responsibility

Reserves collected to guarantee a merchant's Visa payment system obligations must be held and controlled by the acquirer.

Acquirers must hold and control reserves that are accumulated and derived from merchant settlement funds or used to guarantee a merchant's payment system obligations to the acquirer. Agents are not permitted to collect, access, or control merchant reserves.

34. FDIC guidelines for bank examiners require the bank to make sure that bank employees responsible for underwriting have appropriate levels of experience and establish adequate policies and controls to substantiate information derived from third parties, including ISOs.

35. The primary risk in the payment system comes from the guarantees that the payment associations require: the acquiring bank is responsible to the consumer and the issuing bank if, for instance, the merchant fails to deliver the goods or services, submits charges that the consumer did not authorize, or suffers a cybersecurity breach leading to unauthorized charges, any one of which could lead to "chargebacks." If an airline goes out of business and travelers need their tickets refunded, the acquiring bank is on the hook. If a lawyer is disbarred and her clients had prepaid by card, the acquiring bank is liable. And of course, if a merchant outright defrauds consumers, the acquiring bank is responsible for the refunds. Getting the money back from the merchant is then the acquiring bank's problem. Thus, just as the issuing bank is taking on credit risk when it hopes that the consumer will pay their credit card bill, the acquiring bank is taking on credit risk when it hopes that the merchant will not incur chargebacks and when it hopes that the merchant will be able to pay any chargeback liability it does incur.

36. One solution acquiring banks have pursued to mitigate their risk exposure is to have their ISOs agree to indemnify them for these risks. It is wise for ISOs like CMS who take on these risks, known within the industry as a "Wholesale" ISO, to invest in extensive risk and underwriting processes to do their due diligence on merchants both when they apply for an

account and on an ongoing basis. Otherwise, the ISO risks chargeback liability to the bank when consumers dispute the merchant's charges.

37. The payment associations and acquiring banks have also tried to mitigate their risk exposure through other means, such as underwriting procedures and standards. Ultimately, like any extension of credit, accepting a merchant involves a professional judgment about the likelihood of loss and the merchant's ability to repay. If the acquiring bank and its ISO underestimate the likelihood of chargebacks or improperly set commission rates or acceptance criteria, they will lose money.

CMS'S RISK AND UNDERWRITING PROCESS

38. As a Wholesale ISO responsible for every last cent of chargeback liability that its acquiring banks incur, CMS understands the critical importance of its in-house underwriting and risk management processes, which perform additional analysis above and beyond the bank's own independent underwriting and risk management processes.

39. CMS has, unfortunately, learned this lesson the hard way: for example, when chargeback levels from one merchant hit much higher levels than CMS ever expected, CMS wound up paying over $392,000 to ensure that the impacted consumers were reimbursed, at a huge loss to CMS's business.

40. As CMS grew and matured, it took aggressive action to strengthen its underwriting and risk management, including terminating of its own volition, and not at its acquiring banks recommendation or demand, any merchant account CMS deemed to have excessive risk exposure from its portfolio between 2011 and 2019. CMS's other actions include strengthening its standards for accepting new merchants, investing in proprietary and third-party tools,

recruiting highly experienced staff to head its risk and underwriting teams, improving training, and updating internal policies.

41. Those actions had a marked effect on CMS's chargeback rates, which have been well below the 1% mark that is generally viewed as the industry standard, both in terms of the count of chargebacks and their dollar value, since 2013. CMS's chargeback rates in 2018, the latest full year in which we have data, were .58% by dollar and .23% by count.

42. CMS uses a number of methods and tools to monitor its merchants and continually assess their creditworthiness, both when they apply for a merchant account with one of CMS's acquiring banks and on an ongoing basis once they have accounts.

43. CMS has detailed underwriting standards, identifying risk factors such as anticipated sales volume, card-not-present transactions (such as online purchases), merchant financial history, and the principal's creditworthiness and financial history. During this process, CMS must trust the veracity of information a potential new merchant provides where information cannot be verified by an outside source, though for other information, it also attempts to confirm the information through third-party sources.

44. CMS also has underwriting checklists that it uses when onboarding new merchants, requiring both information submitted by the merchant and separate investigative work by underwriting staff. For example, CMS often reviews, among other things, two years of tax returns, certificates of incorporation, business licenses, business websites, credit reports, write-ups from sales representatives, three months of statements from prior processors, voided checks, samples of marketing materials, searches of MasterCard's MATCH (Member Alert to Control High Risk) system recording merchants who have had prior accounts terminated, and Better Business Bureau and other consumer reports. Particular industries may require additional

documentation, such as FDCPA training materials for collections merchants or documentation of clearly-disclosed contact information and return policies on websites for e-commerce merchants (since chargebacks are often a result of customers being unable to work out how to complain directly to the merchant). CMS maintains printouts of all the documents it reviews during the diligence process in its merchant files.

45. These requirements imposed at CMS's initial underwriting stage are much more stringent than those mandated by payment associations like Visa and MasterCard, and in many cases even more stringent than the payment associations' encouraged "best practice" information elements.

46. Based on these underwriting standards, CMS has declined approximately 16% of applications since 2013. Numerous merchants have also withdrawn applications before the underwriting process was completed because CMS's underwriting process was more rigorous than they expected.

47. CMS subscribes to costly merchant monitoring tools considered to be the gold standard in the industry, such as G2 and TSYS Fraud, to identify suspicious payment activity, fraud, and other indications that a merchant is a potential problem.

48. CMS also has tools that allow it to track related accounts when one merchant or multiple merchants with a common principal have more than one merchant account, such as when a merchant has multiple locations, processes transactions both at a physical location and online, or uses different trade names or subsidiaries to sell different products.

49. CMS, in partnership with its acquiring banks, frequently imposes processing limits on its merchants and requires a portion of merchant deposits to be set aside as collateral in reserve accounts in the event of chargebacks or fraud.

50. CMS actively monitors merchants' chargebacks, and requires merchants to participate in chargeback reduction programs when their chargebacks reach specific thresholds. Such thresholds established by CMS have been set at levels well below the thresholds set by the payment association guidelines.

51. CMS may also impose penalties on its merchants for chargebacks above a certain level, which is in addition to the industry-standard fees for each chargeback. This is not viewed as a revenue opportunity for CMS, but rather a financial penalty to encourage merchants to reduce and prevent chargebacks. Thus, CMS's merchants are further incentivized (beyond the industry-standard fees and the banks' practice of setting off chargeback liability against future receipts) to avoid the types of behavior that often results in chargebacks.

52. CMS's Risk Department monitors risk metrics on a daily basis, reporting on merchants that have higher-than-expected or extraordinary processing volumes or chargebacks to management on a weekly basis. The Risk Department also analyzes compilations of monthly processing statistics and metrics for the top 100 merchant accounts and merchant accounts with an increased level of risk. The acquiring banks with which CMS works also have real-time access to the proprietary system CMS uses to track account information, C-Force, which the banks can use to view and create reports of information about the accounts held with those banks, such as the level of chargebacks.

53. To detect fraud by e-commerce vendors, CMS subscribes to third-party website monitoring services and reviews reports from the MasterCard Merchant Online Status Tracking (MOST) system. MOST tracks merchants terminated because of excessive fraudulent activity and screens registrations against databases of terminated merchants, including matches by owner name, address, social security number, EIN, and D&B number.

54. CMS also undergoes regular and rigorous audits by both its acquiring banks and payment associations such as Visa and MasterCard, and uses the results of those audits to further strengthen its underwriting and risk management processes. CMS is also in continual dialog with its acquiring banks and in some cases payment associations regarding industries associated with increased chargeback rates, and has tightened its underwriting standards for particular industries as the payments industry has identified them as emerging areas of concern.

55. Notably, CMS was investing in these measures long before it received its first CID from the FTC. And they were working: based on CMS's continuous active monitoring of its merchants' activity, it terminated more than 90% of merchants responsive to the FTC's CID that were sued by the FTC before the FTC sued the merchant.

"OPERATION CHOKEPOINT" AND THE FTC

56. Between 2012 and 2017, the Consumer Protection Branch of the United States Department of Justice conducted a wide-ranging investigative and enforcement effort it dubbed "Operation Chokepoint," targeting payment system participants including banks and ISOs for allegedly permitting merchants to initiate unauthorized transactions. While "Operation Chokepoint" led to enforcement action against some egregious bad actors, it attracted widespread concern from Congress that Department of Justice and banking regulators would push banks to cut off certain categories of legitimate business from the banking system altogether, or that it would result in higher prices due to payment system participants charging higher fees to merchants in categories disfavored by regulators to cover the increased risk. In response to those concerns arising out of "Operation Chokepoint," the House of Representatives passed a bill with a bipartisan, lopsided 395 to 2 vote that would have restricted banking regulators from requiring banks to categorically restrict service to particular industries, although the abandonment of "Operation Chokepoint" mooted the matter.

57. The FTC, however, has continued to target payments system participants notwithstanding the criticism that "Operation Chokepoint" received, under the theory that certain vaguely-defined acts or omissions by non-bank participants in the payments system (like ISOs) constitute unfair trade practices.

58. Based on this theory, the FTC routinely sends multiple CIDs to ISOs and other payments system participants seeking documents, interrogatory responses, and deposition testimony, frequently about dozens or hundreds of merchants at a time.

59. Based on the discovery it receives in response to CIDs, the FTC's staff then regularly threatens ISOs with liability for every dollar that a merchant has ever processed—even though, as an ISO, the only money that they ever so much as touched was the residual they received and arguably the collateral posted in a merchant's reserve account—unless they agree to drop *every* client in entire categories of wholly lawful business. Approximately 25 ISOs have been forced into these types of settlements by the FTC's threats.

60. When called to testify before Congress about whether the FTC was quietly continuing "Operation Chokepoint," despite it being abandoned by the Department of Justice, the Director of the FTC Bureau of Consumer Protection denied it, stating under oath:

a. "The FTC doesn't intend to impose on payment processors the responsibility to police their customers"

b. "We sue payment processors sparingly and only where we have powerful evidence of their complicity in the underlying fraud."

c. "We don't target our enforcement activity based on high-risk merchants."

d. "[W]e're not pushing the envelope here."

61. As demonstrated by CMS's experience with the FTC summarized below, however, the FTC has not stayed true to these statements or its governing legal standards with respect to its actions and threats vis-à-vis CMS.

THE FTC'S INVESTIGATION OF CMS AND THREATENED COMPLAINT

62. The FTC issued a CID to CMS on August 18, 2017, principally seeking information regarding whether CMS had ever had any accounts for a list of entities or individuals that had been subject to enforcement action by the FTC, SEC, or state attorneys general.

63. For more than two years, CMS has cooperated with the FTC's investigation, repeatedly supplementing its interrogatory responses, producing over 475,000 pages of documents, and producing three current and former executive officers to provide testimony to the FTC staff.

64. The evidence provided to the FTC unequivocally shows CMS's robust underwriting and risk management practices, which have unquestionably strengthened as the company grew and matured. Among other things:

a. CMS declined applications for 21 merchants responsive to the CID ("responsive merchants").

b. Responsive merchants were 3% of CMS's total merchants in 2011, declining to only 0.5% in 2016 and 0.08% in 2017.

c. By 2016 and 2017, less than 0.1% of CMS's processing volume was for responsive merchants.

d. The overwhelming majority of responsive merchants were terminated by CMS before any regulator filed a complaint or subpoenaed CMS—in many cases, several years before.

e. Of the 37 responsive merchants later involved in FTC enforcement actions, CMS had terminated 34 prior to the time of suit.

65. Nonetheless, the FTC's staff apparently were not satisfied. On February 4, 2019, the FTC staff informed CMS that they planned to recommend enforcement action and sent CMS's counsel a proposed complaint and consent order.

66. The proposed complaint's theory is that CMS "failed to adequately screen and monitor its merchant-clients," and thereby misled the banks for whom it acts as a sales organization, a theory that on its face is inconsistent with Director Smith's sworn testimony that "[t]he FTC doesn't intend to impose on payment processors the responsibility to police their customers."

67. The proposed complaint doubles down on its contradiction of Director Smith by alleging the following theories of unfairness:

a. Open[ing] or maintain[ing] payment processing accounts for merchants when the merchants in whose names the accounts were opened were not the merchants processing payments through the accounts;

b. Open[ing] or maintain[ing] payment processing accounts for merchants when the accounts were not being used to process sales of the products indicated in the account applications; or

c. Open[ing] or maintain[ing] payment processing accounts for merchants when the merchants were using the accounts for load balancing, which, among other things, enabled the accounts to avoid triggering chargeback monitoring systems.

68. Directly contrary to Director Smith's testimony, these theories do *not* allege "complicity in the underlying fraud"—rather, they allege that when merchants lie to and violate their promises to CMS, the acquiring bank, and the payment networks, that nonetheless it is an unfair act or practice for CMS to solicit sales, and for the acquiring bank to then open or maintain those

accounts, regardless of what CMS knew or did not then know about the merchants' conduct. That is precisely the "responsibility to police their customers" that Director Smith denied that the FTC was seeking to impose.

69. Compounding the conflict with Director Smith's representations to Congress, both the proposed complaint and proposed consent order pervasively identify broad categories of merchants as high-risk and imply that processing for those broad categories of business is itself suspect.

70. The complaint uses the phrase "high risk" multiple times, identifying industries such as "sales force coaching" and "multi-level marketers" as falling within that category of merchants. That cannot be squared with Director Smith's testimony that "[w]e don't target our enforcement activity based on high-risk merchants."

71. Further demonstrating that the FTC considers certain lawful industries to be inherently suspect and unworthy of having access to the financial system, the Staff's initial proposed consent order directed CMS to:

a. Terminate all businesses that use telephones to induce the purchase of goods or services;

b. Terminate all businesses that represented that their goods or services would help consumers earn income from home, obtain training or education on how to establish a business or make money from a business, obtain employment for an upfront fee, or obtain government grants or government income, benefits, or scholarships;

c. Terminate all businesses that involve a subscription model where consumers have to tell the business to cancel their subscription (that is, every subscription product);

d. Engage in heightened screening of "High Risk Client[s]," a category defined as covering any merchant with more than 15% card-not-present transactions, more than $200,000 in card-not-present transactions a year, or any merchant that sells:

   i. Discount buying clubs;
   ii. Foreclosure protection or guarantees;
   iii. Lottery sales or sweepstakes;
   iv. Medical discount benefits packages;
   v. Multi-level marketing distribution;
   vi. Nutraceuticals (a category that includes vitamins);
   vii. Payment aggregators;
   viii. Cryptocurrency;
   ix. Third party payment processors;
   x. Penny auctions;
   xi. Real estate seminars and training programs; and
   xii. Computer technical support services.

72. Thus, under the FTC's first proposal:

a. CMS would not be able to solicit Amazon as a merchant, because it sells books by Princeton Review about how to get scholarships for college;

b. CMS would not be able to solicit Brigham Young University as a merchant, because it has a business school that represents that its services can assist students in starting or running a business;

c. CMS would have to subject CVS or Walmart to heightened scrutiny, because they sell multivitamins;

d. CMS would have to subject Best Buy or Apple to heightened scrutiny, because the Geek Squad and the Genius Bar provide computer technical support services.

73. The message to millions of merchants could not be clearer: the FTC considers their businesses inherently suspect, and believes that the payment industry would be engaged in unfair acts and practices if it did not subject their applications and accounts to heightened scrutiny. CMS is caught up in this abuse of power, subject to threats that it must acquiesce to heightened scrutiny or not do business with hugely overbroad categories of merchants.

74. While the FTC narrowed some of the categories in response to comments from CMS's attorneys pointing out their dramatic overbreadth, the FTC indicated that it would insist on a ban on serving businesses that fall into certain categories, including any company (like Amazon) who sells nutraceuticals with an option to purchase via subscription (like Amazon's "Subscribe and Save" program). The FTC also kept the list of suspect categories requiring heightened scrutiny and monitoring virtually identical apart from moving subscriptions (for all products *other* than nutraceuticals, which would still be subject to the outright ban), the business-related education and grants categories, and businesses that use telephones to induce sales from the categories subject to an outright ban to one requiring heightened scrutiny. The FTC rejected any further proposal to narrow these categories. And the FTC sought to set the threshold for chargebacks

(which would trigger a duty to "immediately" investigate) at just 55 chargebacks per month, a level well below even the "early warning" thresholds set by the card brand guidelines. What's more, the FTC's various draft orders have all sought to impose a "strict liability" standard—meaning that CMS could be in violation of the terms of the order *without any knowledge of the facts giving rise to that liability*. This is not what the law intends and is far beyond any reasonable bounds of the FTC's authority.

75. The FTC's proposed complaint is replete with allegations of vaguely-defined violations yet wholly devoid of any real substance or support.

76. Most of the complaint's allegations relate to merchants that CMS terminated years ago; in fact, the FTC complains about CMS's chargeback rate *a decade ago*, just a year after it was founded, while ignoring the enormous reduction in chargebacks between then and now.

77. To create the appearance of support for its complaint, the FTC cherry picks quotes from a 2016 report created at the request of one of CMS's acquiring banks. The FTC quotes this report liberally, yet never mentions that the representative at Chesapeake Bank, the very same bank who requested this report to be compiled, submitted an affidavit to the FTC stating that they considered the report's assertions unsubstantiated, already in the process of being addressed, or simply wrong, and that the bank no longer uses that consultant.

78. The FTC similarly ignores the numerous inspection and audit reports for acquiring banks, payment associations, and certification organizations that *approved* of CMS's underwriting and risk management policies and confirmed by sampling merchant files that CMS's actual practices matched its policies.

79. The proposed complaint focuses primarily on three groups of merchants that collectively amounted to 0.25% of CMS's volume during the relevant time period:

a. Apply Knowledge, a business coaching company that CMS terminated in early 2014 due to its high chargeback rates—before the FTC took action against that merchant;

b. Tarr, a company that both sold supplements and performed fulfillment services for several other supplements companies, which CMS dropped as a client in January 2016, more than 18 months before the FTC sued that merchant; and

c. Amkey/USFIA, a group of companies that went from running a lucrative supplements and online auction business to selling unregistered cryptocurrency securities, whose accounts CMS terminated in 2015 after an auditor became suspicious of its business practices—several months before the Securities and Exchange Commission acted to shut down that business.

80. The fact that the FTC could only identify such a minute number of dishonest merchants after two years of investigation and hindsight as their primary tool speaks volumes about the lack of merit of the FTC's purported claims against CMS.

81. Even for this tiny fraction of merchants, moreover, the FTC is stretching.

82. Take Apply Knowledge, for example. The FTC contends that CMS should have re-underwritten Apply Knowledge after learning that Apply Knowledge had retained third-party sales agents to promote its services and those agents were processing through Apply Knowledge's merchant account, a common sales practice that is not per se problematic. But the FTC ignores that the acquiring bank, which has sole responsibility for deciding whether to process payments for each merchant, was aware of the use of third-party sales agents but chose

not to request more information. The FTC also focuses on a drop-shipping services LLC formed by the wife and business partner of Apply Knowledge's principal, which the FTC claims was an attempt to evade bank scrutiny. But it ignores that the supporting documentation (such as joint tax returns, emails that included the spouse, and other relevant documents) clearly showed the relationship between the husband and wife and that the bank clearly had no difficulty identifying the accounts as related.

83. The Tarr-related merchants affirmatively show CMS taking compliance seriously: CMS parted ways with its former CEO, Jack Wilson, after feedback from one of its acquiring banks. When the Tarr accounts were terminated, the stated reason was high chargeback volumes across all its accounts, demonstrating that CMS was actively monitoring merchants based on card brand guidelines, and was able to identify problem merchants, even if the merchant had more than one account.

84. As for Amkey/USFIA, the FTC alleges that CMS provided "false information" to the bank in summaries of the merchant's responses to certain questions. That merchant, however, lied to CMS and supplied forged invoices to CMS to frustrate CMS's and the bank's efforts to discover its wrongdoing—which led to over $392,000 in unrecovered chargeback liability for CMS. In other words, CMS was a *victim* of this fraud—not a party that should be responsible for it.

85. After seeing the FTC's draft complaint, CMS pointed out that these merchants had all been onboarded by its acquiring bank many years ago, and that these merchants had already been terminated by CMS many years ago as well.

86. To avoid the obvious implication that the FTC had no real basis on which to complain about CMS's actual business practices, the FTC amended its draft complaint, adding allegations

about a single more recent merchant, a technical support company called Elite IT. Elite IT had been referred to CMS by the sales representative at the ISO Elite IT had used for many years. CMS was unaware of any concerns with the merchant—Elite IT's prior ISO only told CMS that its acquiring bank could no longer process payments for Elite IT due to a policy change. Unbeknownst to CMS, that was a lie. In fact, Elite IT had been terminated by its acquiring bank for high chargebacks. CMS identified the chargebacks from transaction histories during its underwriting process nonetheless, and agreed to underwrite the account prior to sending the application to its acquiring bank for final approval only on the condition that Elite IT enroll in a chargeback management program to reduce their chargebacks substantially. The FTC later sued Elite IT based on reports that it was making deceptive sales calls to seniors. But notably, the FTC's draft complaint nowhere alleges that CMS had any knowledge of Elite IT's fraudulent conduct.

87. The FTC's accusations of misleading acquiring banks, moreover, runs headlong into an obvious problem: the two banks that the FTC accuses CMS of misleading still work with and are actively seeking more business from CMS. One of those banks even supplied an affidavit *in support of CMS* to the FTC during its investigation.

88. The FTC's allegations, in short, smack of an attempt to justify the sunk cost of two years of investigation by dredging a decade of history to try to find *anything* that might serve as the basis of a claim. They amount to, at best, a few bad apples that CMS has properly addressed. Perhaps with the benefit of hindsight, those bad apples could have been caught earlier or avoided altogether by either CMS or its acquiring bank, but there is no evidence that CMS was knowingly complicit in the merchants' misconduct.

89. Put simply, the FTC's proposed consent orders have sought to impose on CMS onerous restrictions that would significantly impact CMS's ability to provide services to broad categories of legitimate businesses and that are not rationally related to the types of conduct about which the FTC purports to be concerned.

90. After over two years of full cooperation with the FTC's burdensome investigative demands, many months of negotiations and the exchange of multiple settlement proposals, on November 12, 2019, CMS sent the FTC yet another draft proposal (a counter proposal to the FTC's October 25, 2019 proposal). That proposal, like CMS's prior proposals, merely sought to reasonably define key terms to avoid hamstringing CMS's business in unintended, unnecessary, and unreasonable ways.

91. On November 22, 2019, the FTC responded by email, indicating that the FTC would not negotiate from CMS's November 12 draft. CMS responded by email, providing explanations for the provisions of its proposal about which the FTC indicated it had questions, and asking for the courtesy of a further response to CMS's November 12, 2019 proposal by December 2, 2019. On December 2, 2019, the FTC responded, again refusing to even consider CMS's latest proposal. CMS, through its counsel, had a follow-up phone conference with the FTC staff attorneys on December 4, 2019. That conference confirmed that the parties are at an impasse.

92. Negotiations have reached a stalemate. An actual case or controversy thus exists between the parties that warrants this Court's intervention.

THE FTC IS OVERSTEPPING ITS STATUTORY AUTHORITY

93. The FTC's investigation and the theories it has asserted ignore or attempt to evade numerous limitations Congress has placed on its powers.

a. Congress expressly prohibited the FTC from impinging on banking regulators' turf by regulating banks. 15 U.S.C. § 45(a)(2). Banking regulators actively regulate banks'

relationships with ISOs. *See, e.g.*, FDIC, *Risk Management Examination Manual for Credit Card Activities*, § XIX (2007). But the FTC takes the position that it may regulate the non-bank agents through which banks do business, and thus claims it can bring its claims against CMS, whose conduct is solely as an agent of its acquiring banks.

b. Congress expressly created a restitution remedy for violation of final administrative cease-and-desist orders or regulations promulgated through a notice-and-comment process to give clear notice of what is prohibited. 15 U.S.C. § 57b(b). But the FTC takes the position that (i) it may obtain disgorgement of gross receipts from CMS for *any* unfair or deceptive act or practice through an action for injunctive relief claim under 15 U.S.C. § 53(b) without giving any prior notice of what it considers unfair whatsoever,[1] and (ii) it may do so regardless of the fact that CMS never actually possesses payments processed for the merchants at issue at any point in the payment process.

c. Under terms of 15 U.S.C. § 53(b), a person must be "violating, or [] about to violate, any provision of law enforced by the Federal Trade Commission" in order for the

---

[1] The Tenth Circuit has held that 15 U.S.C. § 53(b)—which codifies section 13(b) of the FTCA—authorizes equitable relief beyond an injunction, including restitution, but there is currently a circuit split on the issue. Precedent in the First, Second, Fourth, Eighth, Ninth, Tenth, and Eleventh—holds that, although 15 U.S.C. § 53(b) by its terms authorizes "injunctions," it should be read to authorize the FTC to seek monetary relief, including restitution. *See FTC v. Direct Mktg. Concepts, Inc.*, 624 F.3d 1, 15 (1st Cir. 2010); *FTC v. Bronson Partners, LLC*, 654 F.3d 359, 365 (2d Cir. 2011); *FTC v. Ross*, 743 F.3d 886, 890-892 (4th Cir. 2014); *FTC v. Sec. Rare Coin & Bullion Corp.*, 931 F.2d 1312, 1314-1315 (8th Cir. 1991); *FTC v. Commerce Planet, Inc.*, 815 F.3d 593, 598 (9th Cir. 2016); *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202 n.6 (10th Cir. 2005); *FTC v. Gem Merch. Corp.*, 87 F.3d 466, 469 (11th Cir. 1996). In *FTC v. Credit 14 Bureau Ctr.*, LLC, 937 F.3d 764, 767 (7th Cir. 2019), the court held that "section 13(b)'s grant of authority to order injunctive relief does not implicitly authorize an award of restitution." Hewing carefully to the statutory language, the Seventh Circuit reasoned that "nothing in the text or structure of the FTCA supports an implied right to restitution in section 13(b), which by its terms authorizes only injunctions." *Id.* at 775. The Supreme Court will soon consider similar language governing the SEC's claimed authority to seek restitution. *Liu v. SEC*, No. 18-1501, 2019 WL 5659111, at *1 (U.S. Nov. 1, 2019).

FTC to obtain injunctive relief. But the FTC's draft complaint against CMS seeks injunctive relief based solely on allegations relating to a sliver of CMS's overall business and merchant relationships that date back years, and sometimes a decade, and provides no allegation even to suggest that CMS is presently violating or about to violate any law whatsoever. Indeed, the draft complaint contains nothing that suggests that CMS's risk and underwriting processes today are anything but robust.

d. Congress limited actions for restitution to a three-year statute of limitations, 15 U.S.C. § 57b(d), and has generally enacted a five-year statute of limitations for actions for penalties, including disgorgement, 28 U.S.C. § 2462. But the FTC takes the position that by instead filing suit under Section 13(b)'s injunctive relief provision, it evades the applicability of *any* statute of limitations—which is precisely what it seeks to do here, against CMS.

e. In response to a number of notorious incidents of FTC overreach, Congress limited the FTC's authority to declare practices as "unfair" based on vague public policy considerations. 15 U.S.C. § 45(n). FTC staff have nonetheless taken the position that they are authorized to create novel forms of vicarious liability for payment systems participants, and is seeking to impose such "novel" theories of liability against CMS.

f. Congress specifically barred the FTC from declaring as "unfair" acts where injury is "reasonably avoidable by consumers themselves." *Id*. At present, the card payment system is set up to guarantee that any aggrieved consumer can easily dispute a charge and receive their money back, with the ISO and acquiring bank liable if a merchant lacks funds to pay the chargeback liability. The FTC ignores that key aspect of the card payment system in seeking to hold CMS liable for "unfair" conduct arising not

from its own actions but the actions of a few dishonest merchants, where consumers themselves have the right and ability to avoid all injury.

94. Moreover, the FTC's asserted theories directly contradict representations it has made to Congress and regulated parties. *Supra* ¶¶ 56-61, 66-70. Due process prohibits the FTC from effectively doing an "about face," by asserting for the first time in litigation, without any notice-or-comment rulemaking or other form of prior notice, and at a minimum equitably estops the FTC from pursuing monetary relief based on its new position.

CAUSES OF ACTION

COUNT I

DECLARATORY AND INJUNCTIVE RELIEF—NO VIOLATION OF 15 U.S.C. § 45(a)

95. Plaintiff realleges and incorporates by reference all of the allegations contained in the preceding paragraphs.

96. As a result of the FTC's repeated threats against CMS asserting that CMS engaged in unfair acts or practices, an actual controversy exists between CMS and the FTC.

97. CMS has not and is not engaged in unfair acts or practices, because:

a. CMS's underwriting and and risk monitoring practices are not likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves, and in any event, any risk is outweighed by the significant countervailing benefits to consumers of convenient, widely-available bankcard payment systems in which ISOs and acquiring banks bear the cost if consumers dispute transactions.

b. CMS has no duty to police its merchants and has not been knowingly complicit in any merchants' misconduct;

c. CMS has no duty to exclude entire categories of lawful businesses from the bankcard payment system; and

d. The FTC lacks authority to regulate banks under the guise of regulating their agents.

98. Accordingly, CMS is entitled to a declaration that it has not violated section 15 U.S.C. § 45(a) and an injunction against any further action by the FTC premised on an alleged violation of 15 U.S.C. § 45(a) arising from the actions at issue in this litigation.

COUNT II

DECLARATORY AND INJUNCTIVE RELIEF—NO VIOLATION OF 15 U.S.C. § 53(b)

99. Plaintiff realleges and incorporates by reference all of the allegations contained in the preceding paragraphs.

100. As a result of the FTC's repeated threats to seek injunctive and other equitable relief under 15 U.S.C. § 53(b), an actual controversy exists between CMS and the FTC.

101. The FTC is not entitled to relief under 15 U.S.C. § 53(b), because:

a. The FTC has not shown that CMS is violating or about to violate 15 U.S.C. § 45(a);

b. The FTC lacks authority to seek an injunction because it has not shown that any violation exists or is likely to recur;

c. The FTC lacks authority to seek other relief because 15 U.S.C. § 53(b) does not permit relief other than an injunction;

d. The statute of limitations for an action for a penalty is five years and has elapsed, or in the alternative, the FTC should not be permitted to evade the

express three-year statute of limitations under the express right of action for restitution under 15 U.S.C. § 57b(b).

102. Accordingly, CMS is entitled to a declaration that the FTC is not entitled to any relief under 15 U.S.C. § 53(b) and an injunction against any action by the FTC premised on a violation of 15 U.S.C. § 53(b).

PRAYER FOR RELIEF

WHEREFORE CMS prays for judgment as follows:

a. A declaration that it has not violated section 15 U.S.C. § 45(a).

b. An injunction against any further action by the FTC premised on an alleged violation of 15 U.S.C. § 45(a) arising from the actions at issue in this litigation.

c. A declaration that the FTC is not entitled to any relief under 15 U.S.C. § 53(b).

d. An injunction against any further action by the FTC premised on a violation of 15 U.S.C. § 53(b) arising from the actions at issue in this litigation.

e. Any further relief to which CMS may be entitled.

DEMAND FOR TRIAL BY JURY

CMS demands a trial by jury on all issues so triable.

DATED this 5th day of December, 2019.

Respectfully submitted,

/s/ Jess M. Krannich

MANNING CURTIS BRADSHAW
& BEDNAR PLLC
Jess M. Krannich (Utah Bar No. 14398)
jkrannich@mc2b.com
136 East South Temple, Suite 1300
Salt Lake City, UT 84111
Telephone: (801) 363-5678
Facsimile: (801) 364-5678

KIRKLAND & ELLIS LLP
Mark C. Holscher (pro hac vice forthcoming)
mark.holscher@kirkland.com
Diana Torres (pro hac vice forthcoming)
diana.torres@kirkland.com
Allison Buchner (pro hac vice forthcoming)
allison.buchner@kirkland.com
Kristin Rose (pro hac vice forthcoming)
kristin.rose@kirkland.com
Matthew Gamsin (pro hac vice forthcoming)
matthew.gamsin@kirkland.com
333 South Hope Street
Los Angeles, CA 90071
Telephone: (213) 680-8169
Facsimile: (213) 680-8500

Attorneys for Plaintiff Complete Merchant Solutions, LLC